JOURNAL OF COMBINATORIAL THEORY, Series A 60, 117–122 (1992)

Note

Covering Bounds for Codes

A. R. CALDERBANK

Mathematical Sciences Research Center, AT & T Bell Laboratoiries, Murray Hill, New Jersey 07974

Communicated by V. Pless

Received March 6, 1990; revised August 27, 1990

Given an $[n, k]R$ code C, and a subcode H of C with codimension j, define $S_H^j(C) = \max_{x \in \mathbb{F}_2^n}\{d(x, H) + d(x, C\backslash H)\}$, and define the j-norm, $S^j(C)$ to be the minimum value of $S_H^j(C)$ as H ranges over the subcodes with codimension j. We prove that if $k/(n+1) > R/(R+1)$, then $S^1(C) \leqslant 2R+1$.

1. INTRODUCTION

Let C be an $[n, k]R$ code, and for $\varepsilon = 0, 1$, and $i = 1, 2, ..., n$, let C_ε^i be the set of codewords $c = (c_1, ..., c_n)$ in C for which $c_i = \varepsilon$. We assume that the ith coordinate is not always zero, so that $|C_0^i| = |C_1^i| = 2^{k-1}$. Graham and Sloane [2] define the *norm* $N_i(C)$ *of* C *with respect to the i-th coordinate by*

$$N_i(C) = \max_{x \in \mathbb{F}_2^n} \{d(x, C_0^i) + d(x, C_1^i)\}. \tag{1}$$

If $N_i(C) \leqslant N$ for at least one coordinate i, then C is said to have norm N. Coordinates i for which $N_i(C) \leqslant N$ are called *acceptable*. We define

$$N(C) = \min_{1 \leqslant i \leqslant n} \{N_i(C)\}, \tag{2}$$

and we shall sometimes refer to $N(C)$ as *the norm* of C. An $[n, k]R$ code C for which $N(C) \leqslant 2R+1$ is said to be *normal.*

If A is an $[n_1, k_1]R_1$ code, and B is an $[n_2, k_2]R_2$ code, then their direct sum $A \oplus B$ is an $[n_1+n_2, k_1+k_2](R_1+R_2)$ code. The main reason for studying normal codes is the *amalgamated direct sum construction* (ADS) of Graham and Sloane. If A and B are normal, then the amalgamated direct sum $A \dot{\oplus} B$ is an $[n_1+n_2-1, k_1+k_2-1]$ code with

0097-3165/92 $3.00

norm $2R_1+2R_2+1$, so that $A \oplus B$ has one fewer coordinate than the direct sum, but the same redundancy, and covering radius not more than R_1+R_2. Figure 1 describes the ADS construction in terms of generator matrices of A and B.

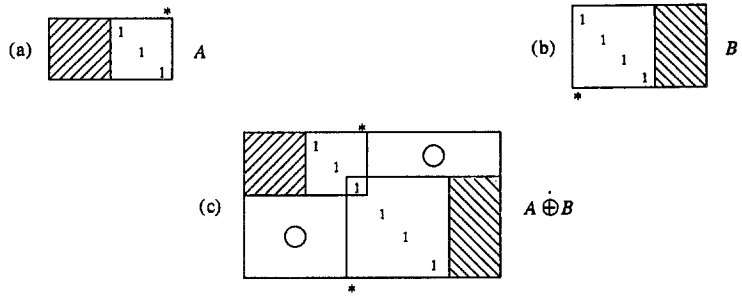

FIG. 1. The amalgamated direct sum (ADS) construction. Choose generator matrices for A, B as shown in (a), (b), where the starred columns are acceptable. A generator matrix for the ADS $A \oplus B$ is shown in (c).

The definition of normality distinguishes n subspaces C_0^i with codimension 1 in C. But given a subspace H of C with codimension j, we may define the *j-norm* $S_H^j(C)$ *of* C *with respect to* H by

$$S_H^j(C) = \max_{x \in \mathbb{F}_2^n} \{d(x, H) + d(x, C \backslash H)\}, \tag{3}$$

so that $N_i(C) = S_{C_0^i}^1(C)$. We define the *j-norm* $S^j(C)$ of C by

$$S^j(C) = \min_H \{S_H^j(C)\}, \tag{4}$$

where the minimum is taken over all subspaces H with codimension j in C. It is very simple to describe the connection between normality and the 1-norm:

THEOREM 1. *There exists an* $[n, k]$ *code with norm* $2R+1$ *if and only if there exists an* $[n-1, k]$ *code with* 1*-norm at most* $2R$.

Proof. Let A be an $[n, k]$ code with norm $2R+1$, and let $A[i]$ be the code obtained from A by puncturing the ith coordinate. If the coordinate i is acceptable, then $S^1(A[i]) \leqslant 2R$. Conversely, let B be an $[n-1, k]$ code, and suppose $S_H^1(B) \leqslant 2R$ for some subspace H of B with codimension 1. Let $B[H]$ be the $[n, k]$ code consisting of all codewords $(b_1, ..., b_n)$, where $(b_1, ..., b_{n-1}) \in B$ and

$$b_n = \begin{cases} 0, & \text{if } (b_1, ..., b_{n-1}) \in H, \\ 1, & \text{otherwise.} \end{cases}$$

Then $N(B[H]) \leqslant 2R+1$, and the nth coordinate is acceptable.

The next example shows that the norm of a code is sometimes greater than the 1-norm.

EXAMPLE 1. Here C is the $[23, 12]3$ Golay code. Then C is normal (with norm $N(C) = 7$) and every coordinate is acceptable. By Theorem 1, $S^1(C[i]) \leqslant 6$ for every i, and equality holds because the covering radius of $C[i]$ is 3. To see that $N(C[i]) = 7$, take any $j \neq i$, and let $c \in C[i]$ be any codeword of weight 6 for which $j \notin \text{supp}(c)$. If $x \in \mathbb{F}_2^{22}$ is (the characteristic vector of) any 3-subset of $\text{supp}(c)$, then $d(x, C_0^j[i]) = 3$, and $d(x, C_1^j[i]) = 4$ so that $N(C[i]) = 7$.

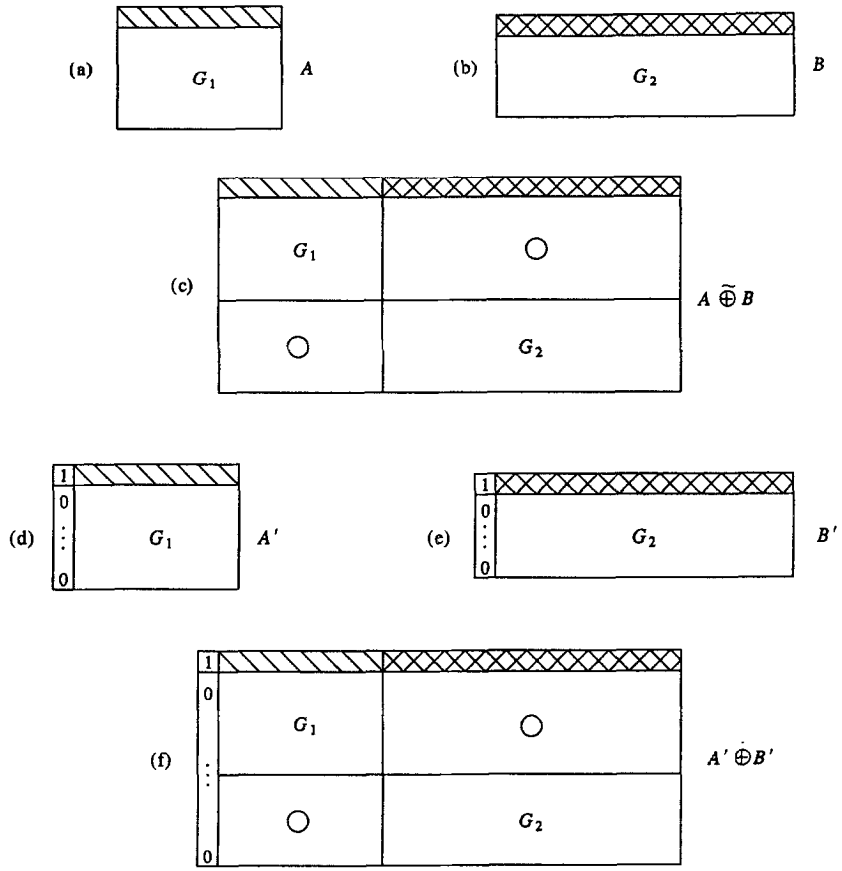

FIG. 2. The subspace direct sum construction (SDS). Choose generator matrices for A, B as shown in (a), (b), where the submatrices G_1, G_2 generate subspaces $H_1 H_2$ for which $S^1_{H_1}(A) = \alpha$, $S^1_{H_2}(B) = \beta$. A generator matrix for the SDS $A \tilde{\oplus} B$ is shown in (c). If $\alpha = 2R_1$, $\beta = 2R_2$, where R_1, R_2 are the covering radii of A, B, then the codes A', B', are normal, and (f) shows a generator matrix for the ADS $A' \dot{\oplus} B'$.

The main reason for studying the 1-norm is the *subspace direct sum construction* (SDS). If A is an $[n_1, k_1]$ code with 1-norm α, and B is an $[n_2, k_2]$ code with 1-norm β, then their SDS $A \tilde{\oplus} B$ is an $[n_1+n_2, k_1+k_2-1]$ code with covering radius at most $\lfloor(\alpha+\beta)/2\rfloor$. Figure 2 describes the SDS construction in terms of generator matrices of A and B, and it describes how to construct a normal $[n_1+n_2+1, k_1+k_2-1]$ code with covering radius $\lfloor(\alpha+\beta+1)/2\rfloor$ from the SDS $A \tilde{\oplus} B$ in certain cases.

Given an $[n, k]R$ code C with $k/(n+1) > R/(R+1)$, a simple counting argument is all that is needed to prove the existence of a subcode H of C with codimension 1 such that $S_H^1(C) \leqslant 2R+1$. The reason that the counting argument works is that every subcode with codimension 1 determines an admissible partition, not just the subcodes C_0^i. This counting argument is presented in Section 2.

2. An Upper Bound on the j-norm of a Code

THEOREM 2. *Let C be an $[n, k]R$ code. If*

$$2^{n-k}(2^{k-\lceil (n-R)/(R+1)\rceil} - 1) < 2^k - 1 \tag{5}$$

then $S_1(C) \leqslant 2R+1$.

Proof. Given a coset $C+y$ with coset leader y, $wt(y) \leqslant R$, let $z_1 = c_1 + y$, $z_2 = c_2 + y$, ..., $z_{l(y)} = c_{l(y)} + y$ be a complete list of coset representatives $z \in C+y$ for which

$$z \neq y \qquad \text{and} \qquad wt(y) + wt(z) \leqslant 2R+1.$$

Let H be a subspace of C with codimension 1. If $x \in C+y$ then either

$$d(x, H) + d(x, C \backslash H) \leqslant 2R+1, \tag{6}$$

or

$$x+y, x+z_1, ..., x+z_{l(y)} \in H, \tag{7}$$

or

$$x+y, x+z_1, ..., x+z_{l(y)} \in C \backslash H. \tag{8}$$

If (6) does not hold then we say that the subspace H *fails to separate the coset* $C+y$. Let $V(y) = \langle c_1, ..., c_{l(y)} \rangle$. Then

$$H \text{ fails to separate } C+y \Leftrightarrow V(y) \subseteq H. \tag{9}$$

Simple counting shows that if

$$\sum_{\text{cosets } C+y} (2^{k-\dim(V(y))}-1) < 2^k - 1$$

then there exists a subspace H with codimension 1 that separates every coset, and $S^1(C) \leqslant 2R+1$ as required. It remains to prove $\dim(V(y)) \geqslant (n-R)/(R+1)$.

There exists a coset $C+y'$ with coset leader y' that is maximal with respect to the property $\text{supp}(y) \subseteq \text{supp}(y')$. Set $y' = y+e$. If $z' = c+y'$, where $c \in C$, and if $wt(y')+wt(z') \leqslant 2R+1$, then $z = z'+e = c+y$ and $wt(y)+wt(z) \leqslant 2R+1$. Thus $\dim(V(y')) \leqslant \dim(V(y))$ and it is sufficient to prove $\dim(V(y')) \geqslant (n-R)/(R+1)$.

Let e_j denote the standard unit coordinate vector. If $j_1 \notin \text{supp}(y')$ then maximality of $\text{supp}(y')$ implies $d(y'+e_{j_1}, C) \leqslant wt(y')$. Let $f_1 = c_1 + y' + e_{j_1}$, where $c_1 \in C$ and $wt(f_1) = d(y'+e_{j_1}, C)$. Then

$$wt(f_1+e_{j_1})+wt(y') \leqslant wt(f_1)+1+wt(y') \leqslant 2wt(y')+1 \leqslant 2R+1.$$

Note that since y' is a coset leader, $j_1 \in \text{supp}(c_1)$. Now take $j_2 \notin \text{supp}(y') \cup \text{supp}(c_1)$ and continue as above. We obtain at least $(n-wt(y'))/(wt(y')+1)$ codewords $c_i \in C$ with the property that

$$(e_{j_i}, c_k) = \begin{cases} 1, & \text{if } i = k, \\ 0, & \text{if } i > k. \end{cases}$$

It follows that

$$\dim(V(y')) \geqslant (n-wt(y'))/(wt(y')+1) \geqslant (n-R)/(R+1).$$

COROLLARY 3. *Let C be an $[n, k]R$ code. If $k/(n+1) > R/(R+1)$ then $S^1(C) \leqslant 2R+1$.*

Proof. If $k > R(n+1)/(R+1)$ then $n-k < (n-R)/(R+1)$ which implies that (5) holds.

Let $t(n, k)$ denote the smallest covering radius of any binary $[n, k]$ code.

COROLLARY 4. *If $k/(n+1) > t(n, k)/(t(n, k)+1)$, then $t(n+2, k) \leqslant t(n, k)+1$.*

Proof. Let $R = t(n, k)$, and let C be an $[n, k]R$ code. If A is the $[2, 1]$ repetition code then the SDS $C \tilde{\oplus} A$ is an $[n+2, k]$ code with covering radius at most $R+1$.

Remarks. (1) Cohen *et al.* [1, Proposition 14], proved that for n large

enough with respect to $n-k$ we have $t(n+2, k) \leqslant t(n, k)+1$. Kilby and Sloane [4] proved that for fixed k and n large enough (that is $k/n \to 0$) we have $t(n+2, k) = t(n, k)+1$.

(2) Honkala [3] considers linear and nonlinear codes and introduces the concept of subnormality: an $(n, k)R$ code C is *subnormal* if there is a subset C_1 of C such that for all $x \in \mathbb{F}_2^n$

$$d(x, C_1) + d(x, C \backslash C_1) \leqslant 2R+1.$$

Theorem 2 shows that linear $[n, k]R$ codes with $k/(n+1) > R/(R+1)$ are subnormal and that C_1 may be taken to be a subcode with codimension 1.

(3) The idea of a subspace direct sum construction also applies to lattices that admit a useful partition into a sublattice of codimension 1 and a translate of that sublattice. Consider for example, the integer lattice $\mathbb{Z}^2$ which is the union of the sublattice $D_2 = \{(a, b) \in \mathbb{Z}^2 \mid a+b \equiv 0 \bmod 2)\}$ and the translate $D_2 + (1, 0)$. It is easy to verify that for any $z \in \mathbb{R}^2$, we have

$$d^2(z, D_2) + d^2(z, D_2 + (0, 1)) \leqslant 1, \tag{10}$$

where $d^2(\ ,\ )$ denotes squared Euclidean distance. Consider the covering radius of the lattice $\Lambda_{2L} = \langle D_2^L, (0101 \ldots 01)\rangle$. It follows from (10) that

$$\begin{aligned} &d^2(z, D_2^L) + d^2(z, D_2^L + (0101 \ldots 01)) \\ &\quad = \left(\sum_{j=1}^{L} d^2(z_i, D_2)\right) + \left(\sum_{j=1}^{L} d^2(z_i, D_2 + (01))\right) \leqslant L \end{aligned}$$

so that either $d^2(z, D_2^L) \leqslant L/2$ or $d^2(z, D_2^L + (0101 \ldots 01)) \leqslant L/2$. Note that the covering radius of $\mathbb{Z}_2^L$ is $L/2$ and that the covering radius of D_2^L is L.

REFERENCES

1. G. D. COHEN, M. R. KARPOVSKY, H. F. MATTSON, JR., AND J. R. SCHATZ, Covering radius—Survey and recent results, *IEEE Trans. Inform. Theory* **IT-31** (1985), 328–343.
2. R. L. GRAHAM AND N. J. A. SLOANE, On the covering radius of codes, *IEEE Trans. Inform. Theory* **IT-31** (1985), 385–401.
3. I. HONKALA, Modified bounds for covering codes, *IEEE Trans. Inform. Theory* **IT-37** (1991), 372–375.
4. K. E. KILBY AND N. J. A. SLOANE, On the covering radius problem for codes, I. Bounds on normalized covering radius, *SIAM J. Algebric Discrete Methods* **8**, No. 4 (1987), 604–618.